



Extreme Doxing

Private investigation

[Hack Forums](#)

MAXIM (UID=3077324)

Introduction

Thank you for purchasing Extreme Doxing. I have been doing some personal work of Private Investigation for the past year and have learnt with the help of Hack Forums. Extreme Doxing is a continued version of my previous guide.

The goal with Extreme Doxing is to cover everything you need to know in order to start your own private investigation service. We will also cover things such as detracing and anonymity. This eBook is also meant to use as a collection of resources.

You may not: leak, share, distribute, sell, resell or in any shape or form share Extreme Doxing with anyone else. You are responsible for your copy which is watermarked with your information. Failure to follow this will result in a community alert together with your information (IP address, email, real name, much more).

Contents

Introduction.....	1
Doxing.....	4
Definitions.....	4
Doxing.....	4
Detracing	4
Anonymity	4
Doxing Template.....	5
Skype.....	6
IP Address	7
Sifting databases	7
IP Logger	8
Finding your target's email address.....	9
Using your target's email address	9
Doxing a HF user	10
Getting an HF users IP	11
House Information.....	12
Obtaining Databases.....	13
Sifting Databases	14
Useful Links.....	16
Detracing	19
Using Google.....	19
Doxing Yourself.....	20
Removing past identities	21
Removing from Google cache.....	22
Removing from lookup sites	23
Checking breaches	24
Removing a dox	25
Faking a dox	26
Anonymity	27
Virtual Private Network	27
Web Browser Choice	28
Email Services	29
Messaging Options	30
Payment Options	31
What Now?.....	32
Leak the dox.....	32

Send an ISP abuse notice	32
Take down Discord server	32
Take down sales pages	32
Closing Words.....	33

Doxing

Definitions

Doxing

Doxing is a technique of tracing someone or gather information about an individual using sources on the internet. Its name is derived from "Documents" or "Docx". Doxing method is based purely on the ability of the hacker to recognize valuable information about his target and use this information to his benefit. It is also based around the idea that, "The more you know about your target, the easier it will be to find his or her flaws"

Detracing

Detracing is the art of removing your tracks. You do what a doxer would do, dox. You find your tracks and you hide them / mislead them / delete them. The latter is the best. There are various of methods but what it almost always comes down to is an "opt-out" option. Site allows you to delete information if it's yours.

Anonymity

Anonymity on the Internet applies to any interaction a user has on the Internet that protects his or her identity from being shared with another user or with a third party. Different levels of anonymity exist, and examples of anonymity can be seen all over the Internet. Some basic examples of anonymity on the Internet include but are not limited to:

- 1) Secure Billing. When a user purchases something with PayPal or on eBay, the user does not reveal his or her personal information to the distributor. Thus, PayPal protects the user's anonymity.
- 2) Question-And-Answer Sites. Users make use of anonymity with sites like Formspring, which allows people to ask anonymous questions of known users, and obtain responses.
- 3) Anonymous Flirting and Networking. Users are able to flirt with others while remaining anonymous. Examples of this include: LikeALittle, Chatroulette, and Omegle.
- 4) Anonymous blogging and posting. Perhaps most importantly or prevalently, users are able to blog anonymously (anonymous Twitter accounts), comment anonymously (on blogspot or Tumblr), or post links anonymously (like on 4Chan).

Doxing Template

So, when doxing, you most likely want a doxing template to parse information you gather. Use a template and save it in a text editor to edit throughout your process of doxing. There are tons templates online; all are pretty much the same. But this is the one I am using:

Personal Information

Full Name:

Date of Birth:

Phone Number:

Email:

Skype:

Facebook:

Twitter:

YouTube:

Other:

Additional

Pictures:

Other:

IP Address:

Hobbies:

Alias(es):

Living

Address:

Landline:

City:

State:

ZIP:

Country:

Occupants:

Flat/House:

Bedrooms:

Optional

Family member:

Date of birth:

Job:

Facebook:

Picture:

Other:

Reason of Dox

Lorem Ipsum

Skype

Deals and such are often dealt over Skype because of its massive communication platform, and things can easily go wrong over there; a currency exchange scam, your partner might try to play you, threats against you or your family, and much more. Knowing how to use your targets Skype in order to dox is crucial to know. Sometimes the best place to start is the least obvious. (If you have your target on Skype) Click on your target's avatar; you will get information such as birth date, gender, language, skype name, phone number, and country.

Birth date: While this is not always correct, considering that most people put fake birth dates, this can potentially be used to compare to another birth date that you parse from another investigation method.

Gender: This is in most cases true, you do not have much use of this information though.

Language: Many people do not put their native language there. Instead, they put English, but in some cases, you will find people having their language set as their native.

Skype name: This is, of course, the most important, will show you below how to use this to parse more information.

Phone number: Believe it or not, but there are people who accidentally set their actual phone number here because they are not aware that it is public.

Country: Not important, it depends on how the language situation is looking.

You mainly want to use that information to compare, not to use for your actual dox and that is because of how unreliable it is; most of the times, the information is fake.

So, moving on to using your victims Skype name; to just Google, the Skype name directly won't get you as far as this command will get you **"skype: username"**.

So, "what can I do with this search" is something you might be wondering, and first of all, if this user is registered here on Hack Forums, and the user have ever made a post saying something like "Hey, add my Skype: *****", then you will be able to find that post with this search, and there you go, you now have his Hack Forums account. You can add that to "Other" in the doxing template. Continuing using only the Skype ID. So, there are something named "Skype resolver", basically it gets the IP-address of your target. Skype resolvers comes and goes, but there are ones that are working as of (November 2017) which are:

- [SkypeGrab](#) (Target has to be **online**)
- [SkypeResolver](#) (Target has to be **online**)

The IP-addresses that you gathered from the Skype resolver is something that you can use. First of all, you can add the IP-address to the template, and secondly, you can use the IP-address to get the location of him. Head over to; IP-tracker.org - enter one IP address a time that you got from "Database records" on your Skype resolver site. Compare every search and then decide which one is probably the one. You will be getting information beyond your imagination! Such as ISP provider, Country, Capital, State, City Location, Postal, Hostname, and much more. Head over to your doxing template, add new tabs and fill in old.

IP Address

With an IP address you can get really far. IP address is the identity of YOU when you are online. That's why you will learn about Virtual Private Networks later on in order to stay anonymous.

What can be done with an IP address?

IP Tracking

Head over to; IP-tracker.org - enter one IP address a time that you got from "Database records" on your Skype resolver site. Compare every search and then decide which one is probably the one. You will be getting information beyond your imagination! Such as ISP provider, Country, Capital, State, City Location, Postal, Hostname, and much more.

Sifting databases

Using your own databases, you can search for the IP address to find accounts connected. With those accounts, you will find IP addresses, usernames, emails, passwords and if you later on logins to the account, you can find even more.

Known database services online

- [We Leak Info](#)
- [LeakBase](#)
- [LeakHub](#)
- [SnusBase](#)
- [LeakedSource](#)

IP Logger

An IP logger is your last go-to. It requires social engineering in order to get your target to click the IP logger. Now, what is an IP logger?

It's basically a link that you generate, and when your target opens that link, it will grab the IP address and store it in a page which you can access using a panel that the site gave you. It's most often just a link which you can bookmark.

You never want to send your target just the IP logger as it is, it must be masked. Which is why you should choose a good IP logger. I highly recommend using [Cyber-Hub](#)

Cyber-Hub's IP logger is the absolute best IP logger that you can find. It can be masked as many known forums such as Hack Forums and Leak Forums.

Save your "IP Logger Key" in order to access the logs later.

Finding your target's email address

Facebook can be a very useful site when it comes to acquiring information, especially someone's email address. Make a simple Google search of your target's real name and see if you can find his or hers Facebook. If they have their details open for everyone, just grab their email from there. When it comes to Facebook, you can also import your contacts through Yahoo to find their email. So, go ahead and create a Yahoo account and on the top left corner where it says "contacts", simply choose Facebook. Login and import the contacts and then you should have their email. Other than that, you can use Skype to your advantage. There are two Skype to Email services that I tend to use:

- [SkypeGrab](#)
- [MostwantedHF](#)

Tip: Sometimes the most obvious place to look is the last place you look. Did your target ever send you any money over PayPal or such site? Check the transaction details for their email.

Using your target's email address

Having your target's email address is definitely one of the better things to have considering that every service online is connected to an email, and some of them display it public for different reasons. There are a few common methods that you can use:

Email to Skype method

1. So, there are two methods to find your target's Skype using Email. The first one, is very basic, just like the mentioned Facebook method above. Head over to Skype and in the "Search" field, enter the email and hit "Search Skype". Simple as that, if your target has a Skype connected with the email you entered, you will find it.
2. The second method to do this is to again use the [MostWantedHF](#) site. Head over to the "Email2Skype" tab and simply enter the email you wish to look up.

PayPal method

Again, very basic yet very effective. Just be careful, this method will include you having to send money, which will tell your information as well. Make sure that you are hidden and safe. So, you have your target's email, simply make a new transaction and send the minimum amount possible (\$0.01), when sent, head over to the main page and click on the transaction. Make sure that you send as "Friends and family".

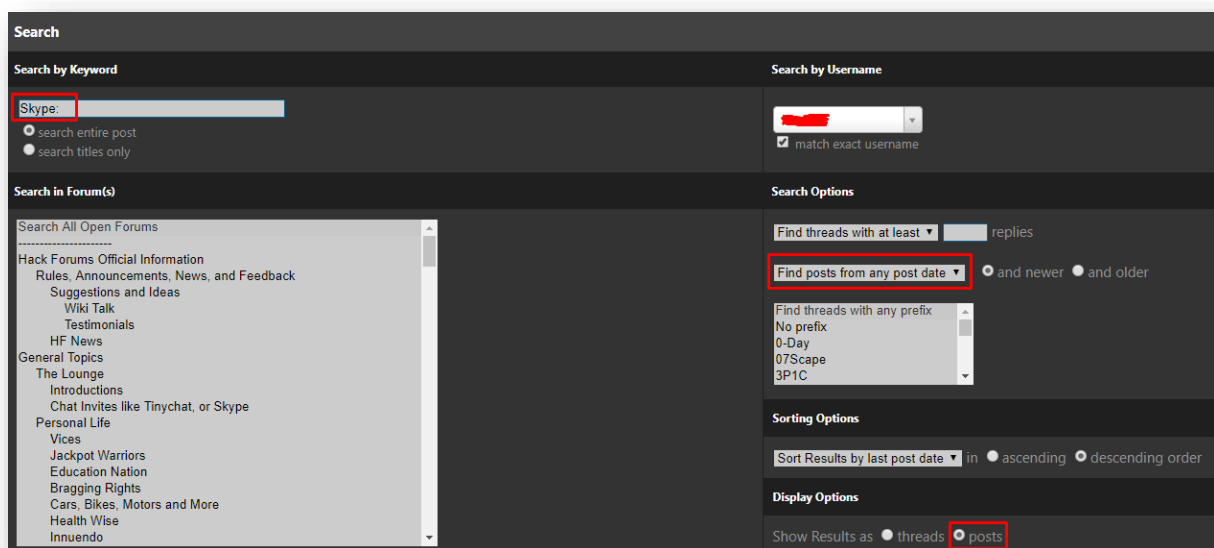
You will get your target's first name and last name using this method.

Doxing a HF user

Many users believe that doxing other Hack Forums users are strictly forbidden, but that is false. You are in fact allowed to dox any HF user you want for any reason. However, you are not allowed to share, leak, spread the dox or anything of that kind on the forum. You are also not allowed to treat or harass any other forum members.

Doxing HF users is fairly easy. The longer the user has been on the forum, the more posts, the more threads etc the user has; the easier to dox.

The [Search](#) function is the key to doxing a HF user.



The screenshot shows the Hack Forums search interface. The 'Search by Keyword' section has a text input field containing 'Skype:' which is highlighted with a red rectangle. Below it are radio buttons for 'search entire post' (selected) and 'search titles only'. The 'Search by Username' section has a text input field with a redacted username and a checked checkbox for 'match exact username'. The 'Search in Forum(s)' section shows a list of forum categories, with 'Search All Open Forums' selected. The 'Search Options' section has a dropdown menu for 'Find threads with at least' set to 'replies', and another dropdown menu for 'Find posts from any post date' which is highlighted with a red rectangle. Below this are radio buttons for 'and newer' (selected) and 'and older'. The 'Sorting Options' section has a dropdown for 'Sort Results by last post date' and radio buttons for 'ascending' and 'descending order'. The 'Display Options' section has radio buttons for 'threads' and 'posts', with 'posts' highlighted by a red rectangle.

Your search term should be "Skype:" / "Skype" / "Discord:" / "Discord" / "Email:" / "Age:"

That way, you will most often find a Skype which is enough for you to get an IP, to sift in databases, to find accounts, emails, usernames, passwords and so on. **Remember to put his or her name in "Search by username"!**

Getting an HF users IP

I previously taught you on how to find the Skype/other contact information on a Hack Forums user, but it's not always that your target has contact information posted public. So, you have to find another way.

There's an IP logging tool named [Grabify](#).

With this tool, you can post an invisible IP logger in one of your threads or posts.

1. Generate your IP logging link "https://grabify.link/IMALOD"
2. Save your Access Link "https://grabify.link/track/02119J"
3. Add MyCode to your IP logging link "[img]https://grabify.link/IMALOD[/img]"
4. Test it out on yourself (by visiting the post/thread. Check the Access Link.
5. Link your target to the post with the invisible IP logging image.

Remember to make it believable on why they should visit your post link.

Make up something that work for your situation and target.

House Information

Using [Zillow](#) and [Realtor](#) you can get information such as; how many baths they have; when the house was built, how big their yard is, how much their house is worth and such. You can also use Google Maps to get a better view where they live. This is something again that you can add to your doxing template, take screenshots and add data.

18008 Newton Ave, NE, Omaha, NE is a single family home that contains 948 sq ft and was built in 1930. It contains 2 bathrooms.

The Zestimate for this house is \$83,504, which has increased by \$1,937 in the last 30 days. The Rent Zestimate for this home is \$1,025/mo, which has increased by \$126/mo in the last 30 days. The property tax in 2016 was \$1,455. The tax assessment in 2016 was \$84,389, an increase of 4.4% over the previous year.

FACTS

- Lot: 6,615 sqft
- Single Family
- Built in 1930
- All time views: 19
- Cooling: Central
- Heating: Forced air

FEATURES

- Parking: Garage - Detached, 600 sqft garage

CONSTRUCTION

- Exterior material: Other
- Roof type: Composition
- Stories: 1

OTHER

- Floor size: 948 sqft
- Parcel #: 0000000000
- Zillow Home ID: 1000421985

Obtaining Databases

We will begin the area that revolves around “databases” with obtaining them. You need to download as many as you possibly can. It’s only a matter of how much space you have on your hard drive. You can obtain them from [Databases.today](#) and simply download all that you can into a folder. Then how to use the databases, will be in the next page.

If you don’t want to obtain your own then you can get a premium account on any of the following sites:

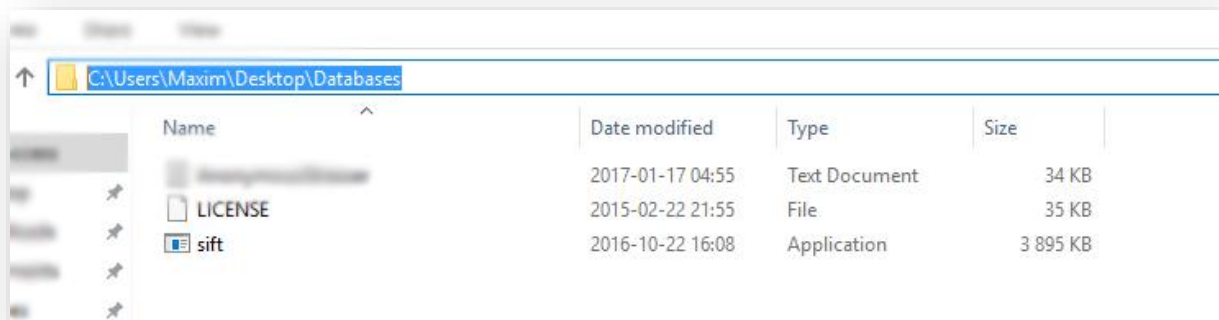
- [We Leak Info](#)
- [LeakBase](#)
- [LeakHub](#)
- [SnusBase](#)
- [LeakedSource](#)

Sifting Databases

First, create a map on your desktop and name “Databases” or whatever you deem fit. Head over to [Sift Tool](#) and download a version that works for your operating system. Then you simply copy Sift.exe and the license file to the folder you created, then add your databases in there. It uses the command prompt to work. So, when you want to search in your databases you need to know some basics of Command Prompt. You created your folder on your desktop, and if you named it “Databases” then this should be your directory

“C:\Users\Maxim\Desktop\Databases” except for “Maxim” which is my computer name.

If you are unsure what your folder directory is named, simply locate it in file explorer and copy the URL.



Copy the URL and head over to Command Prompt. Type “CMD” in your start menu and run as administrator. Once in CMD, you need to change your directory. You do that by typing “cd C:\Users\Maxim\Desktop\Databases”.

```
C:\Users\Maxim\Desktop\Databases>
```

Now to use Sift-tool you enter a new command: **sift hacker** - Where “hacker” is the user you want to look up. Sift tool will scan through your databases for all users with the name “hacker” or where “hacker” is used pretty much anywhere.

```
C:\Users\Maxim>cd C:\Users\Maxim\Desktop\Databases
C:\Users\Maxim\Desktop\Databases>sift hacker
Databases\1.txt: ...hacker...
Databases\2.txt: ...hacker...
Databases\3.txt: ...hacker...
Databases\4.txt: ...hacker...
```

Time for colored logs (to make it easier to see).

Now, what would be cool to have? You guessed it right, colors. Head over to [ANSICON](#) and click the “ANSICON v1.66” or whatever version is the latest. Download it and extract it to a folder on your desktop. Head back to your Command Prompt and change your directory to the Ansicon folder on your desktop. Make sure it sets to either x64 or x86 depending on what you have. You can use the same method as we did before. Open up file explorer and copy the URL. Mine in this case is:

```
C:\Users\Maxim\Desktop\Ansicon\x64
```

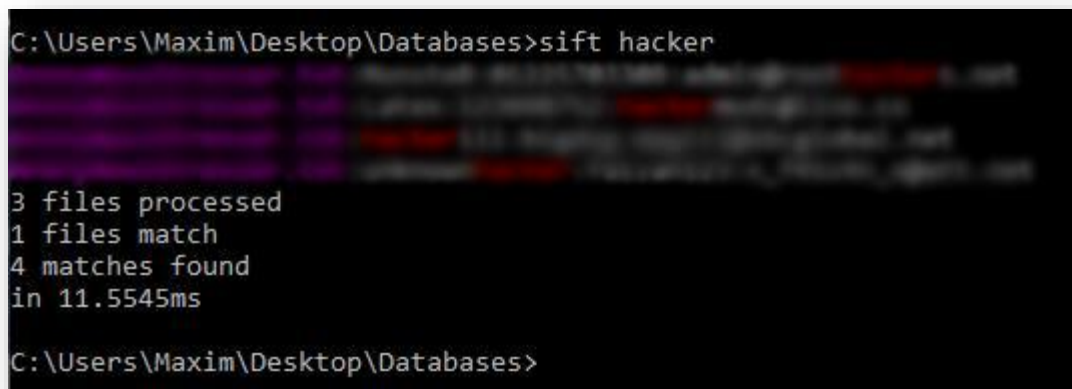
Now you want to install Ansicon and you do that by running aniscon.exe in your Command Prompt by using:

```
ansicon.exe -i
```

Change back your directory to the database folder. Just like we did earlier. Then type in the command:

```
sift -ria --color --err-skip-line-length --stats --write-config
```

Try running the same Sift command as we did earlier. “Sift hacker”, this time, we will have colors. As you can see, it highlights the database name and the keyword that we entered, which was “hacker”. If you want to learn more about Sift commands, click [here](#).



```
C:\Users\Maxim\Desktop\Databases>sift hacker
3 files processed
1 files match
4 matches found
in 11.5545ms
C:\Users\Maxim\Desktop\Databases>
```


Useful Links

Website Lookup

<https://who.is/>
<http://www.whois.com/>

Dox Release

<https://skidpaste.org/>
<http://pastebin.com/>
<http://www.paste.org/p/home>
<https://ghostbin.com/>

IP Address

<http://www.ip-tracker.org/>
<http://ipaddress.com/>
<http://mostwantedhf.info/>
<http://10digits.us>

USA People Search

<http://10digits.us>
<http://www.whitepages.com>
<http://www.411.com>
<http://www.zabasearch.com>
<http://www.intelius.com>
<http://www.yellowpages.com>
<http://publicrecords.directory/>
<http://www.411locate.com>
<http://www.addresses.com>
<http://www.spokeo.com>
<http://www.anywho.com>
<http://www.peoplefinders.com>
<http://www.skipease.com>
<https://www.vetfriends.com/>
<http://radaris.com>
<http://www.superpages.com>
<http://www.advancedbackgroundchecks.com/>
<https://nuwber.com/>

UK People Search

<https://www.gov.uk/electoral-register/overview>
<http://www.192.com>
<http://webmii.com>
<http://www.kgbpeople.com>

<http://www.yasni.com>
http://www.peakyou.com/united_kingdom
<http://britishphonebook.com/>

Canada People Search

<http://www.canada411.ca>
http://www.freeality.com/whitepages_ca.htm
<http://world.192.com/north-america/canada>

Picture Search

<http://www.tineye.com>
<https://images.google.com/>
<http://exifdata.com/>
<http://geoimgr.com/>

Passwords

<https://haveibeenpwned.com/>
<https://www.hacked-db.com/>
<http://www.hashkiller.co.uk/md5-decrypter.aspx>
<https://hacked-emails.com>
<https://breachalarm.com/>
<https://lastpass.com/adobe/>

Phone information and Lookups

<https://nuwber.com/>
<http://reversemobile.com/>
<http://thatsthem.com/>
<http://www.spydialer.com/>
<http://www.phonevalidator.com>
<http://www.fonefinder.net>

Username Search

https://www.google.com/advanced_search
<https://pipl.com>
<http://checkusernames.com>
<http://knowem.com>

Picture Search

<http://www.tineye.com>
<https://images.google.com/>
<http://exifdata.com/>
<http://geoimgr.com/>

Email Search

<http://com.lullar.com>
<http://www.emailfinder.com>
<http://www.spokeo.com/email-search>
<http://ctrlq.org/google/images/>
<http://emailchange.com/>

Other

<http://iknowwhatyoudownload.com/en/peer/>
<http://www.criminalsearches.com>
<http://www.abika.com>

Detracing

Using Google

There is a tool that Google provides which will remove Outdated content from Google and all cached result and snippet will be removed. Note that this will not work on every link you request to have removed, there must be a reason, outdated content. You can do that here:

<https://www.google.com/webmasters/tools/removals?pli=1>

But what if you want to remove *personal information or content with legal issues* as Google describes it, they offer to do it here:

<https://support.google.com/legal/troubleshooter/1114905>

It is a longer process but it works most of the times.

Remove outdated content

Instructions:

- This request works only for pages/images that have **already been modified, or removed from the web**.
- If you need to remove **personal information or content with legal issues**, you should submit [this request instead](#).
- Enter the URL copied from **Google Search Results**.
- **If successful**, cached result and snippet will be removed from Google Search results.
- **If unsuccessful**, [learn why](#).

[More details](#)

Example URL:

REQUEST REMOVAL

Doxing Yourself

The best step when it comes to de-tracing is to attempt to dox yourself with the methods above, see what you can find, you can start by looking at your Skype, enter the following string:

Skype: *SkypeUsername*

This will find any posts or such where you have written for example "Add my Skype: username". Then if you have any posts that are on Hack Forums, you can delete those posts etcetera. If you do not have access to deleting the posts, try looking into upgrading (on Hack Forums - in order to be able to delete posts). But my point is that you will want to put yourself in the seat of someone attempting to dox you. You want to remove every trace that could help them.

Removing past identities

Removing your past accounts is vital to staying off the Radar, I would remove anything that contains your real name and real information here are some links to help you remove your accounts:

- [Facebook](#)
- [Gmail](#)
- [Twitter](#)
- [Myspace](#)
- [Hotmail](#)
- [Skype](#)

There's almost always an option for account deactivation or to delete it complete.

Removing from Google cache

You can ask Google to remove your sensitive personal information, like your bank account number, or an image of your handwritten signature, or a nude or sexually explicit image or video of you that's been shared without your consent, from Google search results.

Now although you have deleted your twitter, Skype, Myspace etc. They can be found in google caches, this is the same with a lot of sites to be honest, I will be going over a known but still working method for removing yourself from Google Cache.

1. Go here: <https://support.google.com/websearch/troubleshooter/3111061?hl=en>
2. Go down to "What do you want to do?" press which one you need.

You have the option of:

Remove information you see in Google Search

Prevent information from showing in Google Search

Click on the one you want, then click the type of removal you need, you will come to a question like "Have you contacted the site's webmaster?" I normally choose the one about removing data under the European data protection act. Then it should bring you to a page, select what type of information you need removing and follow the questions it normally takes around 3-5 Business days depending to remove your requested information.

Removing from lookup sites

There are so many websites that show if you have been breached on any websites and they allow premium users to view this information like emails, addresses, relatives, criminal records, online accounts. I will show you some methods to remove some of your information as I said I am not going in depth with detracing.

LeakBase [Opt Out] click on begin removal process enter your email if it's your email that has been leaked on here otherwise enter your name or IP. They will send a confirmation to your email and you're done.

>> <https://leakbase.pw/removal.php>

Spokeo [Opt Out] First find your information and copy the URL then click on the hyperlink above and paste the URL in the first box then enter your email address they will send you an email for confirmation then you're done.

>> <https://www.spokeo.com/optout>

Peekyou [Opt Out] Self-explanatory fill out the form.

>> <https://www.peakyou.com/about/contact/optout/>

Pipl [Email] Send an email to privacy@pipl.com about requesting information deletion.

>> <https://pipl.com/corp/contact-us/>

ThatsThem [Annoying Form] Self Explanatory

>> <https://thatsthem.com/optout>

Checking breaches

Use the following sites below to see if any of your information has been breached, the way this happens is when someone hacks a website 9/10 they are likely to produce a database dump, 100s are dumped every week so I would keep up to date with this you can use the following sites for checking this.

LeakBase - Database Search, Searches over 1 million databases, just input your name, email, IP or phone number to check if any of your information has been breached on any websites.

>> <https://leakbase.pw/>

HaveiBeenPwned - Enter your username or email address.

If you have been breached I would change your password immediately or just delete that email and start fresh and avoid those sites although you can't exactly predict when a database is going to be dumped but better to be safe than sorry.

>> <https://haveibeenpwned.com/>

Removing a dox

Doxes which are posted on sites such as pastebin can be removed with ease. It is all about what you type when reporting the dox. When it comes to pastebin, you can remove your dox by first of all go to the dox, then click at the "Report abuse" button and file the complaint. It usually takes 3-5 business days in order to get a reply or to have it removed. When filing your complaint, you need to express your concerns and act like people are harassing you. You can type something like this:

Hello, there is a pastebin with sensitive and private information on me. I have had people who have been harassing me for days now and people are treating me now when they have my private information. Please remove this from your site, I can't use the internet properly when this is public.

Faking a dox

In order to mislead people who are trying to gather information about you, you can create a fake dox. First of all, head over to [fakenamegenerator](#).

and make a fake identity. Then you want to post it as you normally would with a dox, but still have some information about yourself such as your most used email and aliases. Maybe include an old Skype to mislead even more.

It should still be posted as any other dox, in a Pastebin etc.

Anonymity

Virtual Private Network

If you are not already using a VPN you should consider using one as it is easy to use and it can be cheap as well. A VPN gives you more control over your privacy, which is a basic human right. It not only hides your internet activity from ISP but also allows you to use public WI-FI without risks. Not only that, it also stops Google from tracking you. Google stores everything, movement, activity, download, etc. Privacy is after all your right and a VPN is, unfortunately, a need. Listen to what other users has to say about VPNs that they use, most important is to use a VPN that does not keep logs. You can look in the VPN Hosting and Services section here on Hack Forums if you find one that fits you. Make sure to read up on it before your purchase. However, my personal recommendation is to use [Mullvad](#). It is ran by a Swedish company and they do not keep logs. They accept Bitcoin, PayPal, Swish, Bank transfer, Bankgiro and they even accept cash to be sent. They have servers in Sweden, and 34 other locations. This is my definitive go-to when it comes to virtual private network. Something that i especially like about them is that they have an auto-connect feature, so that you do not have to bother with connecting yourself every time you turn on your PC. This is taken from Mullvad's site:

Stay secure on public WiFi

Connecting to WiFi at a cafe, hotel, airport, or any other open network means you are at risk for being hacked or tracked. Protect your web browsing with Mullvad in which traffic to and from your computer is encrypted to the highest standards.

Protect against mass surveillance

Worried about your online activity being scrutinized? Mullvad protects your internet traffic from eavesdropping.

Keep your privacy

Your IP address is hidden and replaced by one of ours, ensuring that your activity and location are not linked to you.

No logging and no tracking on our homepage

We don't log traffic on our website and refrain from sending usage statistics to external parties. Our website uses only two cookies: one that keeps you logged in to your account and one that remembers your language preference.

Web Browser Choice

The go-to browser when it comes to helping you staying anonymous online is Tor Browser without a doubt.

>> <https://www.torproject.org/projects/torbrowser.html.en>

The Tor software protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, it prevents the sites you visit from learning your physical location, and it lets you access sites which are blocked.

Tor Browser lets you use Tor on Windows, Mac OS X, or Linux without needing to install any software. It can run off a USB flash drive, comes with a pre-configured web browser to protect your anonymity, and is self-contained (portable)."

But if you want something more user-friendly you can go with Firefox

>> <https://www.mozilla.org/>

you can read more about the reason "why" here:

>> <https://hackforums.net/showthread.php?tid=5377222>

Email Services

There are two right away that I can recommend which are:

Protonmail

>> <https://protonmail.com/>

Tutanota

>> <https://tutanota.com/>

where both are excellent for security and privacy. Both offers encryption of course.

Automatic Email Security

All emails are secured automatically with end-to-end encryption. This means even we cannot decrypt and read your emails. As a result, your encrypted emails cannot be shared with third parties.

Anonymous Email

Protect Your Privacy

No personal information is required to create your secure email account. By default, we do not keep any IP logs which can be linked to your anonymous email account. Your privacy comes first.

Messaging Options

To start off, do not use Skype without a VPN. Skype resolvers are back. These are confirmed to be working: Skypegrab.net & Skyperesolver.net, and they also store the IP of the lookup in a database, the only requirement is that the Skype user is online. If you have been using your Skype without a VPN, I suggest you to junk that one and make a new, and this time use a VPN.

If you rather feel like junking Skype entirely and use a more secure messaging option you can go for TorChat which is encrypted. But something more commonly used is Discord and XMPP.

Discord

>> <https://discordapp.com/>

XMPP

>> <https://hacker.im/register> (Account registration)

>> <https://www.pidgin.im/> (Client for the account)

Payment Options

Obviously, PayPal is a big no-no here as it displays your name and email when sending and receiving a payment. Using cryptocurrency is a much better option and especially if you go with Bitcoin as it is very popular. With Bitcoin you do not have to provide any personal information such as your address, name, number, street name. You can read this article on how to stay anonymously with Bitcoin:

>> <http://cryptorials.io/how-to-use-bitcoin-anonymously/>

What Now?

Let's say that you get scammed online, they should be expected to be doxed then; you can use the dox to get back what you lost. You are honestly only limited by your imagination. This is what you can theoretically do:

Leak the dox

You can leak the dox for other people to use the information provided. The most common way to leak is through Pastebin and such. Here are the most common ones:

1. [Pastee](#)
2. [Pasted](#)
3. [Hastebin](#)
4. [Chop](#)
5. [Pastebin](#)
6. [Ghostbin](#)

Send an ISP abuse notice

If you have your target's IP address and you go to IP-tracker sites and then basically send an abuse notice to his hosting provider. Here are some commonly used IP-tracker sites:

1. [IP-tracker](#)
2. [IPaddress](#)
3. [IP-lookup](#)

Take down Discord server

Does your target host a Discord server that breaks Discord's terms of service?

Take it down [here](#).

Take down sales pages

Does your target sell a product that breaks the terms of service of the market site?

[Selly sales pages can be reported here.](#)

[Rocketr sales pages can be reported here.](#)

Closing Words

Notice

These were all the methods of Extreme Doxing. If you'd like any more information regarding these methods send me a private message on Hack Forums. Make sure to always use the latest version of this eBook in order to get all working methods.

Terms of Service

1. Do not leak this eBook or you will risk a scam report and fraudulent strike report.
2. Chargebacks will result in limitation of your account and a scam report will be opened. Any information that i have (such as real name, IP address, email and much more) can be posted on the deal dispute thread on Hack Forums.

Information storage

All information is stored securely and on a 256-bit encrypted server hosted by Rocketr. We may post your information public if a chargeback occurs. We will never share information if nothing is terminated.